McDermott
Will&Emery

Boston Brussels Chicago Düsseldorf Houston London Los Angeles Miami Milan
Munich New York Orange County Rome San Diego Silicon Valley Washington, D.C.
Strategic alliance with MWE China Law Offices (Shanghai)

FACSIMILE

Date: June 10, 2009 **Time Sent:**

'10 JUN 10 am11:21

To:	Company:	Facsimile No:	Telephone No:
Examiner Melvin Pollack	U.S. Patent and Trademark Office	571-273-3887 040	571-272-3887

From:	Marc E. Brown	*Direct Phone:*	+1 310 788 1569
E-Mail:	meb@mwe.com	*Direct Fax:*	+1 310 277 4730
Sent By:	DeAnna Rodriguez	*Direct Phone:*	+1 310 788 1591
Client/Matter/Tkpr:	028080-0107-06806	*Original to Follow by Mail:*	No
		Number of Pages, Including Cover:	11

Re: U.S. Patent Application Serial No. 10/632,249

Message:
Please see Request for Examiner Interview and draft claim amendments, herewith.

Main Facsimile: +1 310 277 4730 Facsimile Operator: +1 310 788 4170

U.S. practice conducted through McDermott Will & Emery LLP.
2049 Century Park East Suite 3800 Los Angeles, California 90067-3218 Telephone: +1 310 277 4110

PTOL-413A (04-09)
Approved for use through 06/30/2009. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Applicant Initiated Interview Request Form

Application No.: 10/632,249 First Named Applicant: TOUCH, Joseph Dean

Examiner: POLLACK, Melvin H. Art Unit: 2445 Status of Application: Pending

Tentative Participants:

(1) Marc E. Brown (2) Joseph D. Touch

(3) _____ (4) _____

Proposed Date of Interview: June 12, 2009 **Proposed Time:** 10:00 AM EST AM/PM

Type of Interview Requested:

(1) [✓] Telephonic (2) [ ] Personal (3) [ ] Video Conference

Exhibit To Be Shown or Demonstrated: [ ] YES [ ] NO

If yes, provide brief description: _____

Issues To Be Discussed

Issues (Rej., Obj., etc)	Claims/ Fig. #s	Prior Art	Discussed	Agreed	Not Agreed
(1)			[ ]	[ ]	[ ]
(2)			[ ]	[ ]	[ ]
(3)			[ ]	[ ]	[ ]
(4)			[ ]	[ ]	[ ]

[ ] Continuation Sheet Attached

Brief Description of Argument to be Presented:

Applicant would like to discuss the patentability of new claims 27-28 as set forth in the attached draft Amendment.

Remarks are also provided.

An interview was conducted on the above-identified application on _____ .

NOTE: This form should be completed by applicant and submitted to the examiner in advance of the interview (see MPEP § 713.01).

This application will not be delayed from issue because of applicant's failure to submit a written record of this interview. Therefore, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible.

Applicant/Applicant's Representative Signature

Marc E. Brown

Typed/Printed Name of Applicant or Representative

28,590

Registration Number, if applicable

Examiner/SPE Signature

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Docket No.: 028080-0107 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: TOUCH, JOSEPH DEAN, et al.

Application No.: 10/632,249 Customer No.: 33401

Filed: August 1, 2003 Confirmation No.: 3302

Group Art Unit: 2145 Examiner: POLLACK, Melvin H.

Title: ROUTABLE NETWORK SUBNET RELOCATION SYSTEMS AND METHODS

CERTIFICATE OF ELECTRONIC TRANSMISSION

I hereby certify that this correspondence is being transmitted electronically to the United States Patent and Trademark Office On June , 2009

DeAnna Rodriguez

DRAFT NEW CLAIMS AND REMARKS IN RESPONSE TO OFFICE ACTION MAILED JANUARY 14, 2009

DRAFT NEW CLAIMS

27. A method for communicating with a plurality of devices behind the private side of a NAT, each through a different publicly routable network address[1], comprising:

issuing a request from a client behind the private side of the NAT to a server on the public side of the NAT for the publicly routable network addresses[2];

delivering the request from the client to the server through the NAT[3];

receiving the publicly routable network addresses at the client from the server through NAT[4];

---

[1] [0029] The present invention provides a system, method and apparatus for making remote a network subnet, and for making remote a block of routable network addresses... In one embodiment, each node on the subnet corresponds to one of the plurality of allocated addresses from the block. Where the Internet is involved, the resources and services in the subnet may be used to provide Internet services to a device on a network (such as a LAN, intranet, etc.) obscured by a firewall, NAT, or other mechanism that impairs global routability.

[0033] In one embodiment, data traffic that is transmitted by some arbitrary node on an unrelated network and intended for a host device on the first set of nodes is forwarded to a corresponding host or location on the remote subnet. Similarly, data that is transmitted from a node on the remote subnet is forwarded to its corresponding device at the first set of nodes. The network subnet in this embodiment may be the collection of nodes at the first location, and the relocated network subnet may be the collection of nodes at the second, remote location. The relocated subnet of this embodiment effectively reproduces the set of nodes at the first location.

[2] [0044] In another embodiment, a subnet lease is performed. In other words, the delegation of the remote subnet is performed on demand. This embodiment adds a lease broker 60 to the system, as illustrated in FIG. 8. Subnet lease includes the following phases. First, tether router 40 contacts lease broker 60 to obtain a leased subnet.

[0046] Generally, the lease process encompasses certain parameters which may be negotiated between server and client. However, the specifics of tunnel establishment may vary widely depending on numerous factors. These design details are not necessary to the practice of the invention. Where a lease broker or rental site is involved, in general (a) the rental site and *the client (such as a tether router)* "agree" to the lease and (b) certain information is ultimately passed to the server (such as the anchor router) such that the server can configure its end of the tunnel . . . .

[0063] Notably, although the anchor and tether routers correspond to the server and client, respectively, in the example above, the anchor router need not be one device. For example, the anchor router may include a plurality of routers and/or computers, etc., and the tether router may include a plurality of routers and/or computers, etc., each for routing packets, performing services, and the like.

[3] [0044] In another embodiment, a subnet lease is performed. In other words, the delegation of the remote subnet is performed on demand. This embodiment adds a lease broker 60 to the system, as illustrated in FIG. 8. Subnet lease includes the following phases. First, tether router 40 contacts lease broker 60 to obtain a leased subnet. This communication is illustrated by line 61....
[0046] Generally, the lease process encompasses certain parameters which may be negotiated between server and client. .... Where a lease broker or rental site is involved, in general (a) the rental site and the client (such as a tether router) "agree" to the lease and (b) certain information is ultimately passed to the server (such as the anchor router) such that the server can configure its end of the tunnel. The client may negotiate certain parameters with the lease broker, including, for example (i) parameters regarding the block of addresses
(such as the number of addresses),...

[4] [0044] In another embodiment, a subnet lease is performed. In other words, the delegation of the remote subnet is performed on demand. This embodiment adds a lease broker 60 to the system, as illustrated in FIG. 8. Subnet lease

(continued...)

configuring a tether router behind the private side of the NAT to associate each of the devices behind the private side of the NAT with at least one of the publicly routable network addresses[5];

configuring a tunnel through the NAT between the tether router and the anchor router through which packets can be exchanged between the tether router and the anchor router without being translated by the NAT[6];

---

includes the following phases. First, tether router 40 contacts lease broker 60 to obtain a leased subnet. This communication is illustrated by line 61....
[0046] Generally, the lease process encompasses certain parameters which may be negotiated between server and client. .... Where a lease broker or rental site is involved, in general (a) the rental site and the client (such as a tether router) "agree" to the lease and (b) certain information is ultimately passed to the server (such as the anchor router) such that the server can configure its end of the tunnel. The client may negotiate certain parameters with the lease broker, including, for example (i) parameters regarding the block of addresses
(such as the number of addresses),...

[5][0044] In another embodiment, a subnet lease is performed. In other words, the delegation of the remote subnet is performed on demand. This embodiment adds a lease broker 60 to the system, as illustrated in FIG. 8. Subnet lease includes the following phases. .... Second, as shown in FIG. 9, tether router 40 and anchor router 20 thereupon connect via link 30, and are configured accordingly to establish new subnet 50. After this phase, services may be installed, or the minimum routing requirements for data to travel between the leased subnet and network 10 may be established...

[0046] Generally, the lease process encompasses certain parameters which may be negotiated between server and client However, the specifics of tunnel establishment may vary widely depending on numerous factors. These design details are not necessary to the practice of the invention. Where a lease broker or rental site is involved, in general (a) the rental site and the client (such as a tether router) "agree" to the lease and (b) certain information is ultimately passed to the server (such as the anchor router) such that the server can configure its end of the tunnel. The client may negotiate certain parameters with the lease broker, including, for example (i) parameters regarding the block of addresses (such as the number of addresses), (ii) parameters concerning the services desired or necessary for the configuration (such as DNS or DHCP services, etc.),...

[6] [0034] FIG. 1 depicts a relocated network subnet. A network 10 is coupled to an anchor router 20. .... Anchor router 20 is connected
to a remote tether router 40 via a link 30. ... Link 30 may be a physical link, such as a dial-up phone line, Ethernet, line-of-sight optical, etc. Alternatively, link 30 may be a virtual link, such as a tunnel. Either way, link 30 provides communication between anchor router 20 and tether router 40. Link 30 may be preconfigured or negotiated on demand.

[0044] In another embodiment, a subnet lease is performed. In other words, the delegation of the remote subnet is performed on demand. This embodiment adds a lease broker 60 to the system, as illustrated in FIG. 8. Subnet lease includes the following phases. First, tether router 40 contacts lease broker 60 to obtain a leased subnet. This communication is illustrated by line 61. Second, as shown in FIG. 9, tether router 40 and anchor router 20 thereupon connect via link 30, and are configured accordingly to establish new subnet 50. After this phase, services may be installed, or the minimum routing requirements for data to travel between the leased subnet and network 10 may be established. The mechanism for establishing a link (such as a tunnel) may be performed by the lease broker.

[0062] Regardless of the specific methodology of tunnel setup, a connection is established between the anchor and tether. The nature of that connection (whether it is secure, etc.) can be dictated by the needs of the application and the network configuration. Because a tunnel is established directly between the server (anchor router) and client (tether router) in the embodiment above, any NAT or other device obscuring network service or otherwise hiding IP address is traversed, and full routability exists between the two devices over the tunnel. Thus, a device on the subnet and/or coupled to the tether router can directly route data to and from a device on the network coupled to the anchor router. In one embodiment, each node that is part of the subnet coupled to the tether router corresponds to a unique IP address, and the subnet corresponds to a block (or portion of the block) of contiguous, fixed, IP addresses that are globally routable.

(continued...)

receiving packets at the tether router from the anchor router encapsulated within the tunnel through the NAT addressed to at least one of the publicly routable network addresses[7]; and

forwarding the received packets from the tether router to the device that is associated within the tether router to the at least one publicly routable network address to which the packets are addressed[8],

whereby communications to the plurality of devices behind the private side of the NAT are effectuated using publicly routable network address[9].

28. [Same as 27, except change "NAT" to "firewall," "private" to "protected," and "public routable" to "unprotected."][10]

(The subnet may also use certain addresses of the block for other purposes such as configuration.)

[7] [0036] The function of the tether router 40 in the most basic embodiment is to route data to and from the relocated subnet 50 via the link 30. Tether router 40 may be composed of a single device, or of a plurality of devices, depending on the implementation. Tether router 40 may transmit data 55 from subnet 50 that is addressed to non-subnet locations back to anchor router 20 over link 30. This function is illustrated in FIG. 2. Data 55 comes from a device in subnet 50 and is routed through tether router 40 over link 30 and
through anchor router 20 to its destination. [0037] Tether router 40 may also transmit data 55 received on link 30 and addressed to a location in subnet 50. This function is shown in FIG. 3. ...

[0040] The function of the anchor router in the most basic embodiment is to route data to and from the network 10 via the link 30. The anchor router 20 effectively acts as the coordination entrypoint for subnet 50 to the rest of the network 10. As with tether router 40, anchor router 20 may consist of a single physical device, or a plurality of devices. Anchor router 20 may perform various functions. First,
referring to FIG. 5, anchor router 20 may transmit data 57 from the rest of network 10 to tether router 40 over link 30. The data 57 may then be delivered to a service, site, or other address on subnet 50.

[0041] Referring to FIG. 6, anchor router 20 may also transmit data 58 received on link 30 to the rest of network 10. The data 58 may be addressed to any node on network 10, or to anchor router 20 itself.

[8] [0038] As shown in FIGS. 1-7, a block of routable network addresses are allocated to the remote subnet 50, as illustrated conceptually by arrow 99. The network addresses in this embodiment may be placed in the routing table of the tether router; however, other means may be used to store the allocated block of network addresses. In this embodiment, the network addresses, or a portion thereof, may be used to correspond or "map" to the collection of nodes 98. Depending on the configuration, certain network addresses of the allocated block may be used for other purposes, such as for identifying services coupled directly or indirectly to tether router 40, for identifying virtual devices for configuration purposes. Not all IP addresses in the allocated block need by actually used.

[9] [0062] .... Thus, a device on the subnet and/or coupled to the tether router can directly route data to and from a device on the network coupled to the anchor router. In one embodiment, each node that is part of the subnet coupled to the tether router corresponds to a unique IP address, and the subnet corresponds to a block (or portion of the block) of contiguous, fixed, IP addresses that are globally routable. (The subnet may also use certain addresses of the block for other purposes such as configuration.)

DRAFT REMARKS

Problem With Earlier Technology

Computers on the Internet require addresses, much like telephones require phone numbers. These addresses fall into two categories: public and private. Public addresses are also called publicly routable addresses, because they can be reached (routed to) from other public addresses. Private addresses are also called unroutable, because they cannot be reached from other public addresses – these addresses do not appear in the routing tables of routers on the public Internet.

Public addresses can be used as both the source and destination of a connection. Computers with public addresses can initiate connections to other computers (e.g., to contact Google with a request to look up). They can also receive connections, so other computers can call them (e.g., host a web server, Internet telephone, or peer-to-peer file sharing software). Due to the limited number of public addresses, it has become common to configure a device (called a Network Address Translator or NAT) with a single public address on its public side, allowing multiple computers to use private addresses hidden behind that device. The NAT translates the addresses (and sometimes other header parameters) of packets between its public and private sides. NATs are commonly integrated into home DSL routers and cable modems.

NATs allow computers from its private side to contact computers on its public side, but not the converse.[11] Private-side computers can 'call out', but they cannot

[10] [0029] The present invention provides a system, method and apparatus for making remote a network subnet, and for making remote a block of routable network addresses... In one embodiment, each node on the subnet corresponds to one of the plurality of allocated addresses from the block. Where the Internet is involved, the resources and services in the subnet may be used to provide Internet services to a device on a network (such as a LAN, intranet, etc.) obscured by a firewall, NAT, or other mechanism that impairs global routability.

[11] A NAT can be configured to send all incoming connections to a single device, or to allow connections with a-priori known parameters to contact particular private devices. However, they cannot generally allow private devices to run independent copies of the same service; i.e., it is not usually possible to run multiple web servers on the private side of the NAT so that they are accessible from the public side.

receive incoming calls, because the translation table is configured by the first outgoing (private to public) packet. This limitation can be an impediment to many modern capabilities, e.g., running a local web server to monitor computer configurations (e.g., as Toshiba does for software upgrades), running independent local web servers (to host various web pages in general), running Internet telephony services, or running peer-to-peer services. Many such systems can require cumbersome mechanisms that handshake through other computers elsewhere on the Internet, rather than "direct dialing" each other as do computers on the public Internet (see U.S. PGPub 2006/0215684 and its included prior art discussion).

A similar effect with protected and unprotected addresses results from the use of a firewall that similarly impairs communication between these groups of addresses.

Invention of New Claims 27 and 28

Claims 27 and 28 more distinctly point out and claim the subject matter which applicant regards as his invention and more clearly define over the applied art. Support for these claims is set forth in the footnotes which appear in the footnotes to them on this draft submission.

New claim 27 is a method for communicating with a plurality of devices behind the private side of a NAT, each through a different publicly routable network address. A request is issued from a client behind the private side of the NAT to a server on the public side of the NAT for the publicly routable network addresses. The request is delivered from the client to the server through the NAT. The publicly routable network addresses is received at the client from the server through NAT. A tether router behind the private side of the NAT is configured to associate each of the devices behind the private side of the NAT with at least one of the publicly routable network addresses. A tunnel is configured through the NAT between the tether router and the anchor router through which packets can be exchanged between the tether router and the anchor router without being translated by the NAT. Packets are received at the tether router from the anchor router encapsulated within the tunnel through the NAT addressed to at least one of the publicly routable network addresses. The received packets are

forwarded from the tether router to the device that is associated within the tether router to the at least one publicly routable network address to which the packets are addressed. The net effect is that communications to the plurality of devices behind the private side of the NAT are effectuated using publicly routable network address.

Claim 28 is the same as claim 27, but recites a firewall as the device which blocks packet traversals in either direction based on packet header or content. "Private" in claim 1 is also replaced with "protected," and "public" in claim 1 is replaced with "unprotected." This terminology is consistent with what is commonly used to describe these devices.

Deficiencies in Applied References

In the least office action, Cheline et al. (7,197,550) and Carrico et al (2003/0135616) were primarily relied upon. However, neither, permit communications of devices behind the private/protected side of a NAT/firewall to be effectuated using publicly routable/unprotected network address, as required by these new claims, either alone of in combination.

Cheline configures a VPN and connects it via a modem 106 to a VPN concentrator 136 through a VPN tunnel to a local network 156. As part of this configuration, Cheline configures firewall 134 and/or NAT function 228 implemented in memory 210 in modem 106. However, Cheline does not disclose a method to traverse either a NAT or a firewall so as to allow communications to a plurality of devices behind the private side of a NAT using publicly routable network addresses – the fundamental function of these new claims.

Carrico does not make up for this fundamental deficiency. Carrico describes a tunnel between either two hosts (two IPsec clients) or between a host (an IPsec client) and a router (IPsec gateway). Carrico does not disclose a tunnel between two routers, such as between a tether router and an anchor router, as required by the new claims.

Carrico also only provides secure tunneling access for a single private IP address – that of the IPsec client on the private side of the NAT (in either of the cases

described). It does not support tunneling for a plurality of publicly addressable/unprotected network addresses, as also required by the new claims.

It would also not be obvious to modify Cheline to use these features of Carrico. Cheline teaches to cooperate with and utilize NATs, while Carrico teaches to avoid their effects. It would not be obvious to combine a method for configuring a NAT with a method of avoiding a NAT (by traversing it). The two approaches are opposed in intent -- Cheline supports the use NATs, whereas Carrico supports avoiding the effect of a NAT. Indeed, it is not even apparent how their respective functions could even be combined into a single harmonious system.

The combination of Cheline and Carrico would also still be far from the invention of these new claims. Even combined, for example, packets would not be received at a tether router from an anchor router encapsulated within a tunnel that traverses a NAT addressed to at least one of the publicly routable network addresses which is associated with one of the devices within the tether router.

LAS99 1733357-1.028080.0107